



FortiClient (Windows) - Release Notes

Version 6.0.1

FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET COOKBOOK

<http://cookbook.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/support-and-training/training.html>

NSE INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://fortiguard.com/>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdocs@fortinet.com



August 21, 2018

FortiClient (Windows) 6.0.1 Release Notes

04-601-498630-20180821

TABLE OF CONTENTS

| | |
|---|-----------|
| Change Log | 5 |
| Introduction | 6 |
| Licensing | 6 |
| Standalone mode | 6 |
| Special Notices | 7 |
| Microsoft Windows updates related to CPU security flaw (Meltdown) | 7 |
| Nested VPN tunnels | 7 |
| SSL VPN 98% issues | 7 |
| Windows notification of AV being disabled | 7 |
| Microsoft Windows server support | 7 |
| Rebranding Tool not supported | 8 |
| What's New in FortiClient (Windows) 6.0.1 | 9 |
| Enhanced FortiClient integration with FortiSandbox scanning | 9 |
| Added support for IPsec IKEv2 | 9 |
| Web Filter behavior when FortiGuard unavailable | 9 |
| Installation Information | 10 |
| Firmware images and tools | 10 |
| Installation options | 11 |
| Upgrading from previous FortiClient versions | 11 |
| Deploying FortiClient upgrades to Windows 7 endpoints via FortiClient EMS | 11 |
| Downgrading to previous versions | 12 |
| Firmware image checksums | 12 |
| Product Integration and Support | 13 |
| FortiClient 6.0.1 support | 13 |
| Language support | 14 |
| Conflicts with third party antivirus products | 15 |
| Resolved Issues | 16 |
| Endpoint Control | 16 |
| Malware Protection | 16 |
| Web Filter | 17 |
| Remote Access | 17 |
| Vulnerability Scan | 17 |
| GUI | 17 |
| Install and upgrade | 18 |
| Known Issues | 19 |
| Malware Protection | 19 |
| Web Filter | 19 |
| Application Firewall | 19 |

| | |
|---------------------------|----|
| Remote Access | 20 |
| Vulnerability Scan | 20 |
| GUI | 20 |
| Install and upgrade | 21 |
| Other | 21 |

Change Log

| Date | Change Description |
|------------|---|
| 2018-07-23 | Initial release of FortiClient (Windows) 6.0.1. |
| 2018-08-03 | Updated Special Notices on page 7 . |
| 2018-08-10 | Updated What's New in FortiClient (Windows) 6.0.1 on page 9 . |
| 2018-08-21 | Updated Installation options on page 11 . |

Introduction

This document provides a summary of enhancements, support information, and installation instructions for FortiClient (Windows) 6.0.1 build 0099.

- [Special Notices](#)
- [What's New in FortiClient \(Windows\) 6.0.1](#)
- [Installation Information](#)
- [Product Integration and Support](#)
- [Resolved Issues](#)
- [Known Issues](#)

Review all sections prior to installing FortiClient.

Licensing

FortiClient offers two licensing modes:

- Standalone mode
- Managed mode

Standalone mode

In standalone mode, FortiClient is not connected to a FortiGate or FortiClient Enterprise Management Server (EMS). In this mode, FortiClient is free for private individuals and commercial businesses to use. No license is required.



Support for FortiClient in standalone mode is provided on the Fortinet Forums (forum.fortinet.com). Phone support is not provided.

Special Notices

Microsoft Windows updates related to CPU security flaw (Meltdown)

Microsoft Windows updates may not occur due to a CPU security flaw (Meltdown) with anti-virus products installed. Please read the customer service bulletin CSB-180105-1 at <https://support.fortinet.com/Information/Bulletin.aspx>. A PDF of the bulletin can be downloaded from the firmware download directory of the Fortinet support site at <https://support.fortinet.com>.

Nested VPN tunnels

Parallel, independent VPN connections to different sites are not supported; however, FortiClient VPN connection may still be established over existing third-party (for example, AT&T Client) VPN connection (nested tunnels).

SSL VPN 98% issues

The new SSL VPN Windows driver, which was first introduced in FortiClient 5.6.0, resolves various SSL VPN connection issues. The new driver will help increase performance by up to 20% and provide a stable VPN connection.

Latency or poor network connectivity can affect the FortiClient SSL VPN connection. To further help avoid timeouts, the login timeout on the FortiGate can be increased to 180 seconds using the following CLI command:

```
configure vpn ssl settings
set login-timeout 180
```

Windows notification of AV being disabled

In FortiClient 6.0.1, FortiClient will notify *Windows Security Center Antivirus is Down* only when FortiClient Antivirus has really stopped running.

Microsoft Windows server support

For Microsoft Windows servers, the AntiVirus and Vulnerability Scan features for FortiClient are supported.

Rebranding Tool not supported

FortiClient (Windows) 6.0.1 does not support the FortiClient Rebranding Tool.

What's New in FortiClient (Windows) 6.0.1

This section identifies the new features and enhancements in FortiClient (Windows) 6.0.1. For more information, see the *FortiClient Administration Guide*.

Enhanced FortiClient integration with FortiSandbox scanning

Through EMS, FortiClient is able to receive a list of valid file types to monitor locally. New files introduced into the local file system with matching file types are sent to the FortiSandbox.

EMS retrieves the list of file types from FortiSandbox. The EMS administrator may create endpoint profiles with predefined or custom lists of file types, and assign the same to endpoint groups.

This feature requires EMS 6.0.1 and FortiSandbox 3.0.0.

Added support for IPsec IKEv2

FortiClient now offers IPsec VPN with Internet Key Exchange version 2 (IKEv2) protocol between itself and the FortiGate. This is in addition to the existing support for IPsec IKEv1.

Web Filter behavior when FortiGuard unavailable

By default, FortiClient now blocks all web traffic when FortiGuard is unreachable. You can also configure FortiClient to allow web traffic when FortiGuard is unreachable using XML configuration.

Installation Information

Firmware images and tools

The following files are available in the firmware image file folder:

| File | Description |
|--------------------------------------|---|
| FortiClientSetup_6.0.xx.xxxx.exe | Standard installer for Microsoft Windows (32-bit) |
| FortiClientSetup_6.0.xx.xxxx.zip | A zip package containing FortiClient.msi and language transforms for Microsoft Windows (32-bit). Some properties of the MSI package can be customized with FortiClient Configurator tool. |
| FortiClientSetup_6.0.xx.xxxx_x64.exe | Standard installer for Microsoft Windows (64-bit) |
| FortiClientSetup_6.0.xx.xxxx_x64.zip | A zip package containing FortiClient.msi and language transforms for Microsoft Windows (64-bit). Some properties of the MSI package can be customized with FortiClient Configurator tool. |
| FortiClientTools_6.0.xx.xxxx.zip | A zip package containing miscellaneous tools, including VPN Automation files |

The following tools and files are available in the FortiClientTools_6.0.xx.xxxx.zip file:

| File | Description |
|-------------------------|--|
| FortiClientVirusCleaner | A virus cleaner |
| OnlineInstaller | This file downloads and installs the latest FortiClient file from the public FDS |
| SSLVPNcmdline | Command line SSL VPN client |
| SupportUtils | Includes diagnostic, uninstallation, and reinstallation tools |
| VPNAutomation | A VPN automation tool |



Please review the following sections prior to installing FortiClient version 6.0.1: [Introduction on page 6](#), [Special Notices on page 7](#), and [Product Integration and Support on page 13](#).

Installation options

When installing FortiClient version 6.0.1, you can choose the setup type that best suits your needs. FortiClient will always install the Fortinet Security Fabric Agent (SFA) feature and enable the Vulnerability Scan feature by default. You can select to install one or more of the following options:

- Secure Remote Access: VPN components (IPsec and SSL) will be installed.
- Advanced Persistent Threat (APT) Components: FortiSandbox detection and quarantine features will be installed.
- Additional Security Features: Select one or more of the following to install them: AntiVirus, Web Filtering, Single Sign On, Application Firewall



It is recommended to not install VPN components on Windows Server systems if not required.

Upgrading from previous FortiClient versions

FortiClient version 6.0.1 supports upgrading from FortiClient versions 5.4 and later.

If you are deploying an upgrade from FortiClient 5.6.2 or earlier versions via FortiClient EMS and the upgrade fails, uninstall FortiClient on the endpoints, then deploy the latest version of FortiClient.

Deploying FortiClient upgrades to Windows 7 endpoints via FortiClient EMS

By default, EMS 6.0.1 uses TLS 1.2 for incoming SSL connections. This may cause deployment of FortiClient to Windows 7 endpoints to fail.

When deploying FortiClient upgrades to Windows 7 endpoints via FortiClient EMS, one of the following steps is necessary to ensure a successful upgrade.

Enabling support for TLS 1.0 and 1.1 in EMS

Ensure the *Enable TLS 1.0/1.1* option is enabled. See the *FortiClient EMS 6.0.1 Administration Guide* for details.

Enabling support for TLS 1.2 in Windows 7

1. Install the Windows Update Hot Fix.

Update to enable TLS 1.1 and TLS 1.2 as a default security protocol in WinHTTP (KB3140245):
<http://www.catalog.update.microsoft.com/search.aspx?q=kb3140245>



If regular Windows Update is enabled by default, this KB is already installed.

2. Create a DWORD registry entry: DefaultSecureProtocols in the path:

- On x86 architecture systems:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp
- On x64 architecture systems:
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp

Set the value to 0x00000A00 to enable both TLS 1.1 and 1.2.

See also <https://support.microsoft.com/en-gb/help/3140245/update-to-enable-tls-1-1-and-tls-1-2-as-a-default-secure-protocols-in>.

Downgrading to previous versions

Downgrading FortiClient version 6.0.1 to previous FortiClient versions is not supported.

Firmware image checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal located at <https://support.fortinet.com>. After logging in, click on *Download > Firmware Image Checksums*, enter the image file name, including the extension, and select *Get Checksum Code*.

Product Integration and Support

FortiClient 6.0.1 support

The following table lists version 6.0.1 product integration and support information.

| | |
|------------------------------------|--|
| Desktop Operating Systems | <ul style="list-style-type: none">• Microsoft Windows 7 (32-bit and 64-bit)• Microsoft Windows 8, 8.1 (32-bit and 64-bit)• Microsoft Windows 10 (32-bit and 64-bit) <p>FortiClient 6.0.1 does not support Microsoft Windows XP and Microsoft Windows Vista.</p> |
| Server Operating Systems | <ul style="list-style-type: none">• Microsoft Windows Server 2008 R2 or newer <p>FortiClient 6.0.1 does not support Windows Server Core.</p> |
| Minimum System Requirements | <ul style="list-style-type: none">• Microsoft Windows compatible computer with Intel processor or equivalent• Compatible operating system and minimum 512MB RAM• 600MB free hard disk space• Native Microsoft TCP/IP communication protocol• Native Microsoft PPP dialer for dial-up connections• Ethernet network interface controller (NIC) for network connections• Wireless adapter for wireless network connections• Adobe Acrobat Reader for viewing FortiClient documentation• Windows Installer MSI installer version 3.0 or later |
| FortiAnalyzer | <ul style="list-style-type: none">• 6.0.0 and later• 5.6.0 and later |
| FortiAuthenticator | <ul style="list-style-type: none">• 4.3.1• 4.3.0• 4.2.1 <p>FortiToken Mobile push notification is not supported for the following versions:</p> <ul style="list-style-type: none">• 4.2.0• 4.1.0 and later• 3.3.0 and later• 3.2.0 and later• 3.1.0 and later• 3.0.0 and later |
| FortiClient EMS | <ul style="list-style-type: none">• 6.0.0 and later |
| FortiManager | <ul style="list-style-type: none">• 6.0.0 and later• 5.6.0 and later |

FortiOS

- 6.0.0 and later
- 5.6.0 and later

Only IPsec VPN and SSL VPN are supported with the following FortiOS versions:

- 5.4.0 and later

FortiSandbox

- 2.5.0 and later

The following version is supported, but may require authorization of FortiClient to be disabled. To disable authorization run the FortiSandbox CLI command:

```
device-authorization -f
```

- 2.4.0 and later

The following supported versions do not offer authorization of FortiClient:

- 2.3.0 and later
- 2.2.0 and later
- 2.1.0

Language support

The following table lists FortiClient language support information.

| Language | Graphical user interface | XML configuration | Documentation |
|-----------------------|--------------------------|-------------------|---------------|
| English | ✓ | ✓ | ✓ |
| Chinese (simplified) | ✓ | | |
| Chinese (traditional) | ✓ | | |
| French (France) | ✓ | | |
| German | ✓ | | |
| Japanese | ✓ | | |
| Korean | ✓ | | |
| Portuguese (Brazil) | ✓ | | |
| Russian | ✓ | | |
| Spanish (Spain) | ✓ | | |

The FortiClient language setting defaults to the regional language setting configured on the client workstation, unless configured in the XML configuration file.

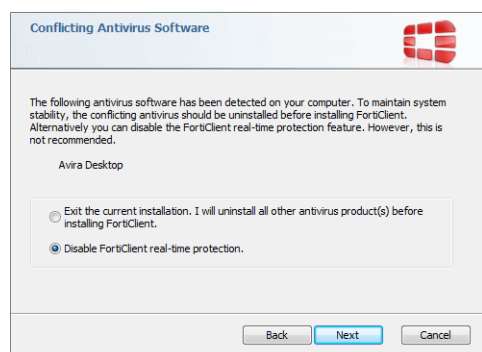


If the client workstation is configured to a regional language setting that is not supported by FortiClient, it defaults to English.

Conflicts with third party antivirus products

The antivirus feature in FortiClient is known to conflict with other similar products in the market. Consider removing other antivirus programs before installing FortiClient.

During a new installation of FortiClient, the installer will search for other registered third party software and, if any is found, warn users to uninstall them before proceeding with the installation. There is also an option to disable FortiClient Real Time Protection (RTP).



Resolved Issues

The following issues have been fixed in version 6.0.1. For inquiries about a particular bug, please contact [Customer Service & Support](#).

Endpoint Control

| Bug ID | Description |
|--------|---|
| 486859 | disable_unregister not working. |
| 488095 | EMS failed to update quarantined files for dual registered endpoint. |
| 489256 | Compliance with third party AV does not work properly. |
| 494232 | FortiClient Console shows <i>Not Participating in Security Fabric</i> . |
| 495917 | FCUnregister not working for 64-bit client. |
| 496759 | Auto group assignment tag rule is broken on FortiClient 6.0.0 GA. |

Malware Protection

| Bug ID | Description |
|--------|---|
| 474472 | Saving images to OneDrive using Snipping Tool triggers AV detection on transient file. |
| 480516 | b1167: FortiClient AV ignoring exclusion list when Windows scheduled task triggers AV scan (system user in session 0) . |
| 487452 | FortiClient 5.6.6 AV Real Time Protection causing third party application called RMS to crash. |
| 491199 | FortiClient Sandbox right-click scan does not quarantine or block malicious file. |
| 492444 | Right-click scan with FortiClient AntiVirus window does not show. |
| 494803 | FortiClient sends empty SN to FortiSandbox during submission. |
| 495539 | FortiClient sends the same file twice/again to FortiSandbox. |
| 497098 | fmon triggers numerous dll load errors. |

Web Filter

| Bug ID | Description |
|--------|--|
| 477771 | Add option to not block "unrated" if FortiGuard cannot be contacted. |
| 492752 | Web Filter cannot be re-enabled in standalone mode without restarting FortiClient. |

Remote Access

| Bug ID | Description |
|--------|---|
| 461136 | FortiClient causing Blue Screen of Death on Windows 10 configured with VLANs (Intel driver 23.1). |
| 483826 | FortiClient sends IPsec SA delete when xauth is not completed in two minutes. |
| 490855 | Shows incorrect VPN profile when connecting from FortiTray. |
| 497346 | FortiClient 6.0: no connection is possible with client certificate. |

Vulnerability Scan

| Bug ID | Description |
|--------|---|
| 496189 | Vulnerability Scan will run about every hour. |

GUI

| Bug ID | Description |
|--------|--|
| 485558 | <i>Fix Now</i> button should be grayed out when there are no vulnerabilities. |
| 489159 | If settings are locked, the <i>Clear</i> button on the <i>Notifications</i> page should be hidden. |
| 489423 | Compliance and Telemetry status to not being translated to system OS. |
| 492210 | Toggling <i>Block malicious websites</i> subcategory will not save the config. |
| 492397 | Connecting VPN from FortiTray should not list certificates. |
| 492647 | Several GUI issues with b62. |

| Bug ID | Description |
|--------|---|
| 495203 | Cannot shutdown a FortiClient which has <i>Password Lock Configuration When Disconnected from EMS</i> enabled in profile. |
| 495209 | Confusing FortiClient status when connection to EMS is down. |
| 495792 | Opening GUI on Swedish OS results in an exception. |
| 495798 | Saving VPN in FortiClient 6.0 cause an error. |
| 496616 | <code>minimize_window_on_connect</code> set to 1 is not working as expected. |
| 496819 | FortiClient 6.0 requires elevated privileges to run the console. |
| 496904 | b0067: Unable to edit AV Malicious Websites settings after editing Web Filter. |

Install and upgrade

| Bug ID | Description |
|--------|---|
| 495604 | Grammar error in FortiClient reboot message. |
| 496724 | FortiClient loses configuration when upgrading from 5.6.6 to 6.0. |
| 496881 | Unable to upgrade or uninstall FortiClient 5.6.6. |

Known Issues

The following issues have been identified in FortiClient (Windows) 6.0.1. For inquiries about a particular bug or to report a bug, please contact [Customer Service & Support](#).

Malware Protection

| Bug ID | Description |
|--------|---|
| 481003 | FortiClient causing longer logon time to terminal server(Citrix) for first user. |
| 483523 | Black screen for a few minutes after login/logoff. |
| 489052 | Memory leak caused by FortiAptFilter.sys. |
| 496084 | AV exclusion list does not work in on-demand scan if %windir% or %systemroot% variables are used. |
| 496326 | FortiClient is sending intermittently files from local disk to the FortiSandbox for analysis. |
| 499891 | Scan on insertion does not work all the time. |

Web Filter

| Bug ID | Description |
|--------|--|
| 489821 | FortiClient 5.6.6 and Windows 8.1 SSL error. |

Application Firewall

| Bug ID | Description |
|--------|---------------------------------------|
| 482920 | FortiClient blocking DF set response. |

Remote Access

| Bug ID | Description |
|--------|---|
| 450245 | Need to add a switch for the number of auto-connect retries. |
| 471234 | Some inconvenience with current per user password design for both SSL and IPsec. |
| 472223 | Unable to select certificate for SSL VPN. |
| 486362 | FortiClient 5.6.6 disables Windows IKE and AuthIP IPsec keying modules when connecting the VPN which effects MS direct access. |
| 491407 | FortiClient auto-connect when off-net not working (IPsec certificate). |
| 495325 | FortiClient 6.0.0 VPN auto connect feature not working properly. |
| 501027 | b0152: FortiClient IPsec VPN IKE version 2 cannot register on IPsec virtual tunnel interface. |
| 501631 | b0154: IKE version 2 FortiClient version cannot establish IPsec VPN tunnel on remote FortiGate when user enables two-factor authentication. |
| 502113 | IKE version 2 config is missing <i>Save Password</i> , <i>Auto Connect</i> , <i>Always Up</i> options for FortiClient 94. |

Vulnerability Scan

| Bug ID | Description |
|--------|--|
| 467328 | FortiClient log for Vulnerability Scan should include file path. |

GUI

| Bug ID | Description |
|--------|---|
| 492890 | FortiClient malware GUI says malware is quarantined when in fact it is not. |

Install and upgrade

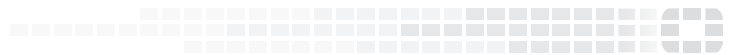
| Bug ID | Description |
|--------|--|
| 496895 | When using EMS to upgrade FortiClient from 5.6 to 6.0.0, installer waits until someone logs in to start. |
| 479229 | After upgrading FortiClient from 5.6.4 to 5.6.6, AV scan history is lost. |
| 496724 | FortiClient loses configuration when upgrading from 5.6.6 to 6.0. |
| 497115 | GUI is blank after installation on Hungarian Windows. |
| 497387 | FortiClient Configurator should support automatic group assignment. |

Other

| Bug ID | Description |
|--------|---|
| 488842 | Total uninstall 6.22.1 completely removing managed FortiClient. |



FORTINET®



Copyright© 2018 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.